

Asymptotic Automorphism Groups of Circulant Graphs and Digraphs

Soumya Bhoumik and Edward Dobson
 Department of Mathematics and Statistics
 Mississippi State University
 Mississippi State, MS 39759 USA

and
 Joy Morris
 Department of Mathematics and Computer Science
 University of Lethbridge
 Lethbridge, AB T1K 3M4 Canada

February 24, 2013

Abstract

We show that almost all circulant graphs have automorphism groups as small as possible. Of the circulant graphs that do not have automorphism group as small as possible, we give some families of integers such that it is not true that almost all circulant graphs whose order lies in any one of these families, are normal. That almost all Cayley (di)graphs whose automorphism group is not as small as possible are normal was conjectured by the second author, so these results provide counterexamples to this conjecture. It is then shown that there is a “large” family of integers for which almost every circulant digraph whose order lies in this family and that does not have automorphism group as small as possible, is normal. We additionally explore the asymptotic behavior of the automorphism groups of circulant (di)graphs that are not normal, and show that no general conclusion can be obtained.

1 Introduction

Determining the full automorphism group of a Cayley (di)graph is one of the most fundamental questions one can ask about a Cayley (di)graph. While it is usually quite difficult to determine the automorphism group of a Cayley (di)graph, characterizing almost all Cayley graphs of a group G , based on the structure of G , has been of consistent interest in the last few decades. Babai, Godsil, Imrich, and Lovász (see [2, Conjecture 2.1]) conjectured that almost all Cayley graphs of any group G that is not generalized dicyclic or abelian with exponent greater than 2 are GRR’s (have automorphism group G_L , the left regular representation of G). A similar conjecture was made for digraphs (with no exceptions) by Babai and Godsil [2]. Babai and Godsil [2, Theorem 2.2] proved these two conjectures for nilpotent (and nonabelian) groups of odd order. In 1998,

Xu [13] introduced the notion of a normal Cayley (di)graph of a group G : a Cayley (di)graph Γ of a group G such that $G_L \triangleleft \text{Aut}(\Gamma)$. Xu also conjectured that for each positive integer n there exists a group G such that almost all Cayley (di)graphs of G are normal Cayley (di)graphs of G (see [13, Conjecture 1] for the precise formulation of this conjecture). In 2010, the second author showed that almost all Cayley graphs of an abelian group G of odd prime-power order are normal [4].

In this paper, we first investigate in Section 3 the proportion of the set of normal circulant (di)graphs in the family of circulant (di)graphs. We show that almost all circulant graphs have automorphism group as small as possible (Theorem 3.1), which make them normal immediately. In [4, Conjecture 4.1], the second author conjectured that almost every Cayley (di)graph whose automorphism group is not as small as possible is a normal Cayley (di)graph. We show that this conjecture fails for circulant digraphs of order n (Theorem 3.4), where $n \equiv 2 \pmod{4}$ has a fixed number of distinct prime factors, and point out some “gaps” in the proof of [4, Theorem 3.5], which leads to additional counterexamples to [4, Conjecture 4.1] for graphs in the case where $n = p$ or p^2 and p is a **safe prime**, i.e. $p = 2q + 1$ where q is prime, or when n is a power of 3 (Theorem 3.5). Finally, we prove that the conjecture holds for digraphs of order n where n is odd and not divisible by 9 (Theorem 3.6). We also show that the conjecture holds for graphs of order n where n is still odd and not divisible by 9, if we add the extra condition that n is not of the form $n = p$ or p^2 where p is a safe prime (Theorem 3.7).

In Section 4, we focus on non-normal circulant (di)graphs. A variety of authors have shown that non-normal Cayley (di)graphs are either generalized wreath products (see Definition 2.6) or have automorphism group that of a deleted wreath product (see Definition 2.15). We show that there exist sets of integers S_1, S_2 , and a family of sets of integers S_c such that almost all non-normal circulant graphs and digraphs whose order is in S_1 have automorphism group that of a deleted wreath product (Theorem 4.2), almost all non-normal circulant graphs and digraphs whose order is in S_2 are generalized wreath products (Theorem 4.3), and neither generalized wreath products nor those graphs whose automorphism group is that of a deleted wreath product of circulant graphs and digraphs dominates amongst those whose order is in any S_c (Theorem 4.1). We remark that we do not know if any set S_c is infinite (but when $c = 2$ for example, S_c consists of all products of twin primes).

In the next section, we will focus on background results and terminology, as well as developing the counting tools needed in Sections 3 and 4.

2 Preliminaries and tools

We start by stating basic definitions, and then proceed to known results in the literature that we will need. We will finish with results that will be the main tools throughout the rest of the paper.

By “almost all” circulant (di)graphs in some family F_1 of circulant (di)graphs of order in a set S of integers being in some family F_2 of circulant (di)graphs, we mean that

$$\lim_{n \in S, n \rightarrow \infty} \frac{|F_2|}{|F_1|} = 1.$$

Definition 2.1 Let G be a group and $S \subset G$ such that $1_G \notin S$. Define a digraph $\Gamma = \Gamma(G, S)$ by $V(\Gamma) = G$ and $E(\Gamma) = \{(u, v) : v^{-1}u \in S\}$. Such a digraph is a *Cayley digraph of G with connection set S* . A Cayley graph of G is defined analogously though we insist that $S = S^{-1} = \{s^{-1} : s \in S\}$. If G is a cyclic group, then a Cayley (di)graph of G is a *circulant (di)graph of order n* , where $|G| = n$.

It is straightforward to verify that for $g \in G$, the map $g_L : G \rightarrow G$ by $g_L(x) = gx$ is an automorphism of Γ . Thus $G_L = \{g_L : g \in G\}$, the left regular representation of G , is a subgroup of the automorphism group of Γ , $\text{Aut}(\Gamma)$.

Definition 2.2 Let G be a transitive permutation group with complete block system \mathcal{B} . By G/\mathcal{B} , we mean the subgroup of $S_{\mathcal{B}}$ induced by the action of G on \mathcal{B} , and by $\text{fix}_G(\mathcal{B})$ the kernel of this action. Thus $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$ where $g/\mathcal{B}(B_1) = B_2$ if and only if $g(B_1) = B_2$, $B_1, B_2 \in \mathcal{B}$, and $\text{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for all } B \in \mathcal{B}\}$.

It is not difficult to show using the fact that a transitive abelian group is regular [11, Proposition 4.4], and that every block system of a permutation group G containing a regular abelian subgroup is formed by the orbits of a normal subgroup of G (in fact, formed by the orbits of a subgroup of a regular abelian subgroup of G). In this paper, the transitive permutation groups that we will encounter will also contain a regular cyclic subgroup, and so every complete block system will be formed by the orbits of a normal subgroup. In fact, a complete block system will always consist of the cosets of a cyclic group [11, Exercise 6.5].

A *vertex-transitive (di)graph* is a (di)graph whose automorphism group acts transitively on the vertices of the (di)graph.

Definition 2.3 Let Γ_1 and Γ_2 be vertex-transitive digraphs. Let

$$E = \{((x, x'), (y, y')) : xy \in E(\Gamma_1), x', y' \in V(\Gamma_2) \text{ or } x = y \text{ and } x'y' \in E(\Gamma_2)\}.$$

Define the *wreath (or lexicographic) product* of Γ_1 and Γ_2 , denoted $\Gamma_1 \wr \Gamma_2$, to be the digraph such that $V(\Gamma_1 \wr \Gamma_2) = V(\Gamma_1) \times V(\Gamma_2)$ and $E(\Gamma_1 \wr \Gamma_2) = E$.

We remark that the wreath product of a circulant digraph of order m and a circulant digraph of order n is circulant. Note that what we have just defined as $\Gamma_1 \wr \Gamma_2$ is sometimes defined as $\Gamma_2 \wr \Gamma_1$, particularly in the work of Praeger, Li, and others from the University of Western Australia.

Definition 2.4 Let Ω be a set and $G \leq S_\Omega$ be transitive. Let G act on $\Omega \times \Omega$ by $g(\omega_1, \omega_2) = (g(\omega_1), g(\omega_2))$ for every $g \in G$ and $\omega_1, \omega_2 \in \Omega$. We define the *2-closure* of G , denoted $G^{(2)}$, to be the largest subgroup of S_Ω whose orbits on $\Omega \times \Omega$ are the same as G 's. Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the orbits of G acting on $\Omega \times \Omega$. Define digraphs $\Gamma_1, \dots, \Gamma_r$ by $V(\Gamma_i) = \Omega$ and $E(\Gamma_i) = \mathcal{O}_i$. Each Γ_i , $1 \leq i \leq r$, is an *orbital digraph* of G , and it is straightforward to show that $G^{(2)} = \cap_{i=1}^r \text{Aut}(\Gamma_i)$. A *generalized orbital digraph* of G is an arc-disjoint union of orbital digraphs of G .

Clearly the automorphism group of a graph or digraph is 2-closed.

The following theorem appears in [9] and is a translation of results that were proven in [6–8] using Schur rings, into group theoretic language. We have re-worded part (1) slightly to clarify the meaning. In the special case of circulant digraphs of square-free order n , an equivalent result was proven independently in [5].

Theorem 2.5 *Let $G \leq S_n$ contain a regular cyclic subgroup $\langle \rho \rangle$. Then one of the following statements holds:*

1. *There exist G_1, \dots, G_r such that $G^{(2)} = G_1 \times \dots \times G_r$, and for each G_i , either $G_i \cong S_{n_i}$, or G_i contains a normal regular cyclic group of order n_i . Furthermore, $r \geq 1$, $\gcd(n_i, n_j) = 1$ for $i \neq j$, and $n = n_1 n_2 \dots n_r$.*
2. *G has a normal subgroup M whose orbits form the complete block system \mathcal{B} of G such that each connected generalized orbital digraph contains a subdigraph Γ which is an orbital digraph of G and has the form $\Gamma = (\Gamma/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle \rho \rangle|$.*

Definition 2.6 A circulant digraph Γ with connection set S is said to be a (K, H) -*generalized wreath circulant digraph* (or just a *generalized wreath circulant digraph*) if there exist groups H, K with $1 < K \leq H \leq \mathbb{Z}_n$ such that $S \setminus H$ is a union of cosets of K .

The name generalized wreath is chosen for these digraphs as if $K = H$, then Γ is in fact a wreath product. We now wish to investigate the relationship between generalized wreath circulant digraphs and the preceding result. We shall have need of the following result.

Lemma 2.7 *Let Γ be a disconnected generalized orbital digraph of a transitive group G . Then the components of Γ form a complete block system \mathcal{B} of G .*

PROOF. As the blocks of $G^{(2)}$ are identical to the blocks of G [10, Theorem 4.11] ([10] is contained in the more accessible [12]), it suffices to show that the set of components \mathcal{B} of Γ is a complete block system of $G^{(2)}$. This is almost immediate as $G^{(2)} = \cap_{i=1}^r \text{Aut}(\Gamma_i)$, where $\Gamma_1, \dots, \Gamma_r$ are all of the orbital digraphs of G . Assume that $\Gamma = \cup_{i=1}^s \Gamma_i$, for some $s \leq r$. Then $\cap_{i=1}^s \text{Aut}(\Gamma_i) \leq \text{Aut}(\Gamma)$, so that \mathcal{B} is a complete block system of $\cap_{i=1}^s \text{Aut}(\Gamma_i)$. Also, $G \leq G^{(2)} = \cap_{i=1}^r \text{Aut}(\Gamma_i) \leq \cap_{i=1}^s \text{Aut}(\Gamma_i)$. Thus \mathcal{B} is a complete block system of $G^{(2)}$ as \mathcal{B} is a complete block system of $\cap_{i=1}^s \text{Aut}(\Gamma_i)$. \square

We will require the following partial order on complete block systems.

Definition 2.8 We say that $\mathcal{B} \preceq \mathcal{C}$ if for every $B \in \mathcal{B}$ there exists $C \in \mathcal{C}$ with $B \subseteq C$. That is, each block of \mathcal{C} is a union of blocks of \mathcal{B} .

Our main tool in examining generalized wreath circulants will be the following result.

Lemma 2.9 *Let G be 2-closed with a normal subgroup M and a regular subgroup $\langle \rho \rangle$. Let \mathcal{B} be the complete block system of G formed by the orbits of M , and suppose that each connected generalized orbital digraph contains a subdigraph Γ which is an orbital digraph of G and has the form $\Gamma = (\Gamma/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle \rho \rangle|$. Then there exists a complete block system $\mathcal{C} \succeq \mathcal{B}$ of G such that $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$.*

PROOF. Observe that we may choose $M = \text{fix}_G(\mathcal{B})$, in which case $|M \cap \langle \rho \rangle| = |B|$, where $B \in \mathcal{B}$, so that b is the size of a block of \mathcal{B} . First suppose that if $B, B' \in \mathcal{B}$, $B \neq B'$, then any orbital digraph Γ' that contains some edge of the form $\vec{x}y$ with $x \in B$, $y \in B'$ has every edge of the form $\vec{x}y$, with $x \in B$, $y \in B'$. It is then not difficult to see that every orbital digraph Γ of G can be written as a wreath product $\Gamma' = \Gamma_1 \wr \Gamma_2$, where Γ_1 is a circulant digraph of order n/b and Γ_2 is a circulant digraph of order b . Then $G/\mathcal{B} \wr \text{fix}_G(\mathcal{B})|_B \leq \text{Aut}(\Gamma')$ for every orbital digraph Γ' , and so $G/\mathcal{B} \wr \text{fix}_G(\mathcal{B})|_B \leq G^{(2)}$. Then result then follows with $\mathcal{C} = \mathcal{B}$. (Note that G is 2-closed, so $G^{(2)} = G$.)

For convenience, we denote the orbital digraph that contains the edge $\vec{x}y$ by Γ_{xy} . We may now assume that there exists some $B, B' \in \mathcal{B}$, $B \neq B'$, and $x \in B$, $y \in B'$ such that Γ_{xy} does not have every edge of the form $\vec{x}'y'$, with $x' \in B$ and $y' \in B'$. Note then that no $\Gamma_{x'y'}$ with $x' \in B$ and $y' \in B'$ has every directed edge from B to B' . Let \mathcal{X} be the set of all Γ_{xy} such that if $x \in B_1 \in \mathcal{B}$ and $y \in B_2 \in \mathcal{B}$, $B_1 \neq B_2$ then Γ_{xy} does not have every edge from B_1 to B_2 . Let $\hat{\Gamma}$ be the generalized orbital digraph whose edges consist of all edges from every orbital digraph in \mathcal{X} , as well as every directed edge contained within a block of \mathcal{B} . Then no orbital digraph that is a subgraph

of $\hat{\Gamma}$ can be written as a connected wreath product $\Gamma' \wr \bar{K}_b$ for some Γ' , and so by hypothesis, $\hat{\Gamma}$ must be disconnected.

By Lemma 2.7, the components of $\hat{\Gamma}$ form a complete block system $\mathcal{C} \succeq \mathcal{B}$ of G . (To see that $\mathcal{C} \succeq \mathcal{B}$, note that $\hat{\Gamma}$ contains every edge from B to B' , so B is in a connected component of $\hat{\Gamma}$. Since G is transitive ($\langle \rho \rangle \leq G$), $\mathcal{C} \succeq \mathcal{B}$.) Let $\Gamma_1, \Gamma_2, \dots, \Gamma_r$ be the orbital digraphs of G , and assume that $\cup_{i=1}^s \Gamma_i = \hat{\Gamma}$. If $1 \leq i \leq s$, then $(G^{(2)}/\mathcal{C})|_{\text{fix}_{G^{(2)}}(\mathcal{C})} \leq \text{Aut}(\Gamma_i)$ as $G^{(2)} \leq \text{Aut}(\Gamma_i)$, Γ_i is disconnected, and each component is contained in a block of \mathcal{C} . Thus $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq \text{Aut}(\Gamma_i)$ for every $1 \leq i \leq s$. If $s+1 \leq i \leq r$, then if $B, B' \in \mathcal{B}$, $B \neq B'$ and $\vec{x}y \in E(\Gamma_i)$ for some $x \in B$, $y \in B'$, then $\vec{x}y \in E(\Gamma_i)$ for every $x \in B$ and $y \in B'$. Also observe that as the subgraph of $\hat{\Gamma}$ induced by B is K_b , the subgraph of Γ_i induced by G is \bar{K}_b . We conclude that Γ_i is the wreath product $\Gamma_i/\mathcal{B} \wr \bar{K}_b$, and so $\text{Aut}(\Gamma_i)$ contains $\text{Aut}(\Gamma_i/\mathcal{B}) \wr S_b$. Then $\text{fix}_{G^{(2)}}(\mathcal{B})|_B \leq \text{Aut}(\Gamma_i)$ for every $B \in \mathcal{B}$. As $\mathcal{B} \preceq \mathcal{C}$, $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq \text{Aut}(\Gamma_i)$ for every $1 \leq i \leq r$ and as $G^{(2)} = \cap_{i=1}^r \text{Aut}(\Gamma_i)$, $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$. \square

Lemma 2.10 *Let Γ be a circulant digraph of order n . Then Γ is a (K, H) -generalized wreath circulant digraph if and only if there exists $G \leq \text{Aut}(\Gamma)$ such that G contains a regular cyclic subgroup, and $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$, where $\mathcal{B} \preceq \mathcal{C}$ are formed by the orbits of K and H , respectively.*

PROOF. Suppose first that $G \leq \text{Aut}(\Gamma)$ with ρ a generator of a regular cyclic subgroup in G , and there exist complete block systems $\mathcal{B} \preceq \mathcal{C}$ of G such that $\text{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)} \leq \text{Aut}(\Gamma)$ for every $C \in \mathcal{C}$. Since $\rho \in G$, the action of $\text{fix}_{G^{(2)}}(\mathcal{B})|_C$ is transitive on every $B \subseteq C$, so between any two blocks $B_1, B_2 \in \mathcal{B}$ that are not contained in a block of \mathcal{C} , we have that there is either every edge from B_1 to B_2 or no edges from B_1 to B_2 . Let \mathcal{B} be formed by the orbits of $K \leq \langle \rho \rangle$. Then for every edge $\vec{x}y$ whose endpoints are not both contained within a block of \mathcal{C} , $(y-x) + K \subset S$. Let \mathcal{C} be formed by the orbits of $H \leq \langle \rho \rangle$. Then $S \setminus H$ is a union of cosets of K as required.

Conversely, if Γ is a (K, H) -generalized wreath circulant, then it is not hard to see that $\rho^m|_C \in \text{Aut}(\Gamma)$ for every $C \in \mathcal{C}$, where ρ generates $(\mathbb{Z}_n)_L$ and $m = [\mathbb{Z}_n : K]$. Let G be the largest subgroup of $\text{Aut}(\Gamma)$ that admits both \mathcal{B} and \mathcal{C} as complete block systems; clearly $\rho \in G$. Also, since $G^{(2)}$ has the same block systems as G and is a subgroup of $\text{Aut}(\Gamma)$, $G^{(2)} = G$. Now, if $g \in \text{fix}_G(\mathcal{B})$, then $g|_C \in \text{Aut}(\Gamma)$ as well. But this implies that $g|_C \in G$ and the result follows. \square

Combining Lemma 2.9 and Lemma 2.10, and recalling that the full automorphism group of a (di)graph is always 2-closed, we have the following result.

Corollary 2.11 *Let Γ be a circulant digraph whose automorphism group $G = \text{Aut}(\Gamma)$ satisfies Theorem 2.5 (2). Then Γ is a generalized wreath circulant digraph.*

We now wish to count the number of generalized wreath circulant digraphs.

Lemma 2.12 *The total number of generalized wreath circulant digraphs of order n is at most*

$$\sum_{p|n} 2^{n/p-1} \left(\sum_{q|(n/p)} 2^{(n-n/p)/q} \right),$$

where p and q are prime.

PROOF. Let Γ be a (K, H) -generalized wreath circulant digraph of order n . By Lemma 2.10, there exists $G \leq \text{Aut}(\Gamma)$ that admits \mathcal{B} and \mathcal{C} such that $\rho \in G$, and $\text{fix}_{G(2)}(\mathcal{B})|_C \leq \text{Aut}(\Gamma)$ for every $C \in \mathcal{C}$, where \mathcal{B} is formed by the orbits of K and \mathcal{C} is formed by the orbits of H (so \mathcal{B} consists of the cosets of K and \mathcal{C} consists of the cosets of H). Let \mathcal{B} consist of m blocks of size k . Then $\rho^m|_C \in \text{Aut}(\Gamma)$ for every $C \in \mathcal{C}$. Choose $q|k$ to be prime, and let $G' \leq \text{Aut}(\Gamma)$ be the largest subgroup of $\text{Aut}(\Gamma)$ that admits a complete block system \mathcal{D} consisting of n/q blocks of size q . Note then that $\rho^{n/q}|_C \in G'$ for every $C \in \mathcal{C}$. Let p be a prime divisor of the number of blocks of \mathcal{C} , and \mathcal{E} the complete block system of $\langle \rho \rangle$ consisting of p blocks of size n/p . Then $\mathcal{C} \preceq \mathcal{E}$ and $\rho^{n/q}|_E \in G'$ for every $E \in \mathcal{E}$. Thus every (K, H) -generalized wreath circulant digraph is a (L_q, M_p) -generalized wreath circulant digraph, where L_q has prime order q where q divides $|K|$ and M_p has order n/p where p divides $n/|H|$. Note that there is a unique subgroup of \mathbb{Z}_n of prime order q for each $q|n$, and that M_p is also the unique subgroup of \mathbb{Z}_n of order n/p .

As $|L_q| = q$, we use the definition of an (L_q, M_p) -generalized wreath circulant digraph to conclude that $S \setminus M_p$ is a union of some subset of the $(n - n/p)/q$ cosets of L_q that are not in M_p . Thus there are $2^{(n-n/p)/q}$ possible choices for the elements of S not in M_p . As there are at most $2^{n/p-1}$ choices for the elements of S contained in M_p , there are at most $2^{n/p-1} \cdot 2^{(n-n/p)/q} = 2^{n/p+n/q-n/(pq)-1}$ choices for S . Summing over every possible choice of q and then p , we see that the number of generalized wreath digraphs is bounded above by

$$\sum_{p|n} 2^{n/p-1} \left(\sum_{q|(n/p)} 2^{(n-n/p)/q} \right)$$

□

Corollary 2.13 *The total number of generalized wreath circulant digraphs of order n is bounded above by $(\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q .*

PROOF. Note that no term in the previous summation given in Lemma 2.12 is larger than $2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of

n/q . As the number of prime divisors of n is at most $\log_2 n$, we have that

$$\sum_{p|n} 2^{n/p-1} \left(\sum_{q|(n/p)} 2^{(n-n/p)/q} \right) \leq (\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}.$$

□

Corollary 2.14 *The total number of generalized wreath circulant graphs of order n is bounded above by $(\log_2^2 n) 2^{n(p+q-1)/(2pq)+1/2}$, where q is the smallest prime dividing n , and p is the smallest prime dividing n/q . So the total number of generalized wreath circulant graphs of order n is at most $(\log_2^2 n) 2^{3n/8+1/2}$.*

PROOF. It is straightforward using Lemma 2.12 and the fact that there are at most two elements that are self-inverse in \mathbb{Z}_n (namely 0 and $n/2$ if n is even, and $0 \notin S$), and at most one coset of \mathbb{Z}_n/L_q that is self-inverse and not in M_p (as \mathbb{Z}_n/L_q is cyclic) to show that the number of generalized wreath circulant graphs of order n is at most

$$\sum_{p|n} 2^{(n/p-2)/2+1} \left(\sum_{q|(n/p)} 2^{((n-n/p)/q-1)/2+1} \right).$$

Note that no term in this sum is larger than $2^{n(p+q-1)/(2pq)+1/2}$, where q is the smallest prime dividing n and p is the smallest prime dividing n/q . Again, as the number of prime divisors of n is at most $\log_2 n$,

$$\sum_{p|n} 2^{(n/p-2)/2+1} \left(\sum_{q|(n/p)} 2^{((n-n/p)/q-1)/2+1} \right) \leq (\log_2^2 n) 2^{n(p+q-1)/(2pq)+1/2}.$$

Now, $(p+q-1)/pq \leq 3/4$. Hence the number of generalized wreath circulant graphs is bounded above by $(\log_2^2 n) 2^{3n/8+1/2}$. □

We now consider digraphs whose automorphism group satisfies Theorem 2.5 (1). Suppose Γ is a circulant digraph of order n , and there exist G_1, \dots, G_r such that for each G_i , either $G_i \cong S_{n_i}$, or G_i contains a normal regular cyclic group of order n_i . Furthermore, $r \geq 1$, $\gcd(n_i, n_j) = 1$ for $i \neq j$, and $n = n_1 n_2 \cdots n_r$. If no $G_i \cong S_{n_i}$ with $n_i \geq 4$, then $\text{Aut}(\Gamma)$ contains a normal regular cyclic group and Γ is a normal circulant digraph.

Definition 2.15 A circulant (di)graph Γ with cyclic regular subgroup $G \cong \mathbb{Z}_n$ is of **deleted wreath type** if there exists some m such that:

- $m \mid n$;

- $\gcd(m, n/m) = 1$; and
- if $H = \langle n/m \rangle$ is the unique subgroup of order m in G , then $S \cap H \in \{\emptyset, H \setminus \{0\}\}$, and for every $g \in \langle m \rangle \setminus \{0\}$, $S \cap (g + H) \in \{\emptyset, \{g\}, (g + H) \setminus \{g\}, g + H\}$. (Notice that because $\gcd(m, n/m) = 1$, the group $\langle m \rangle$ contains precisely one representative of each coset of H in G .)

A circulant digraph is said to be of **strictly deleted wreath type** if it is of deleted wreath type and is not a generalized wreath circulant.

Clearly a strictly deleted wreath type circulant is a deleted wreath type circulant, but there are deleted wreath type circulants which are not strictly deleted wreath type. For an example of the latter, consider a circulant digraph on pqm vertices where $m \geq 4$ and p, q and m are relatively prime, whose connection set is $S = (\langle pq \rangle \setminus \{0\}) \cup (m + \langle mq \rangle)$. If we let $H = \langle q \rangle$ and $K = \langle mq \rangle$, then this digraph is an (H, K) -generalized wreath circulant. And if we let $H = \langle pq \rangle$ then $S \cap H = H \setminus \{0\}$, while for $g \in \langle m \rangle \setminus \{0\}$, we have $S \cap (g + H) = \{g\}$ if $g \in m + \langle mq \rangle$ and $S \cap (g + H) = \emptyset$ otherwise, so this digraph is of deleted wreath type.

The name deleted wreath type is chosen as these digraphs have automorphism groups that are isomorphic to the automorphism groups of deleted wreath products (see [9] for the definition of deleted wreath product digraphs). We now study the automorphism groups of deleted wreath type circulant digraphs.

Lemma 2.16 *Let Γ be a circulant digraph on \mathbb{Z}_n , and let $m \geq 4$ be a divisor of n such that $\gcd(m, n/m) = 1$. Then Γ is of deleted wreath type with m being the divisor of n that satisfies the conditions of that definition, if and only if $\text{Aut}(\Gamma)$ contains a subgroup isomorphic to $H \times S_m$ with the canonical action, for some 2-closed group H with $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$.*

PROOF. In this proof for a given m satisfying $n = km$ and $\gcd(m, k) = 1$, it will be convenient to consider $\mathbb{Z}_n = \mathbb{Z}_k \times \mathbb{Z}_m$ in the obvious fashion. The sets $B_i = \{(i, j) : j \in \mathbb{Z}_m\}$ for each $i \in \mathbb{Z}_k$ will be important.

First, suppose Γ is of deleted wreath type with $m \geq 4$ being the divisor of n that satisfies the conditions of that definition, and $n = mk$. Using $\mathbb{Z}_n = \mathbb{Z}_k \times \mathbb{Z}_m$, we see that for every $i \in \mathbb{Z}_k \setminus \{0\}$, we have $S \cap B_i \in \{\emptyset, \{(i, 0)\}, B_i \setminus \{(i, 0)\}, B_i\}$. Also, $S \cap B_0 \in \{\emptyset, B_0 \setminus \{(0, 0)\}\}$.

Let \mathcal{B} be the partition of $\mathbb{Z}_k \times \mathbb{Z}_m$ given by $\mathcal{B} = \cup_{i \in \mathbb{Z}_k} B_i$. Let G be the maximal subgroup of $\text{Aut}(\Gamma)$ that admits \mathcal{B} as a complete block system. Clearly the canonical regular cyclic subgroup isomorphic to $\mathbb{Z}_n = \mathbb{Z}_k \times \mathbb{Z}_m$ admits \mathcal{B} , so is a subgroup of G .

Define $H \leq S_k$ to be the projection of G onto the first coordinate. Since $\mathbb{Z}_k \times \mathbb{Z}_m \leq G$, clearly $\mathbb{Z}_k \leq H$. We claim that $H \times S_m \leq \text{Aut}(\Gamma)$. To see this, we consider the action of any element of

this group, on any arc of Γ .

Let $((i_1, j_1), (i_2, j_2))$ be an arc of Γ , and let $(h, g) \in H \times S_m$. Suppose first that $i_1 = i_2$. We have $S \cap B_0 \in \{\emptyset, B_0 \setminus \{(0, 0)\}\}$, and $i_1 = i_2$ forces $S \cap B_0 \neq \emptyset$. Hence the subgraph of Γ induced by the vertices of any B_i is complete, so clearly $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is an arc since $h(i_2) = h(i_1)$.

Now suppose $i_1 \neq i_2$. So $h(i_1) \neq h(i_2)$. Let $i = i_2 - i_1$ and let $i' = h(i_2) - h(i_1)$, with $1 \leq i, i' \leq k - 1$. Notice that since H is the projection of G onto the first coordinate, there is some $g \in G$ that takes B_{i_1} to $B_{h(i_1)}$ and B_{i_2} to $B_{h(i_2)}$. Hence the number of arcs in Γ from B_{i_1} to B_{i_2} must be the same as the number of arcs from $B_{h(i_1)}$ to $B_{h(i_2)}$. Now, the number of arcs in Γ from B_{i_1} to B_{i_2} is $|S \cap B_i|$, while the number of arcs in Γ from $B_{h(i_1)}$ to $B_{h(i_2)}$ is $|S \cap B_{i'}|$, so these values must be equal. Since $1 \leq i, i' \leq k - 1$, both of these sets have the same cardinality from $\{0, 1, m - 1, m\}$; in fact, since $((i_1, j_1), (i_2, j_2))$ is an arc of Γ , the cardinality cannot be 0. Since $m \geq 4 > 2$ these cardinalities are all distinct, so $S \cap B_i$ and $S \cap B_{i'}$ are uniquely determined by their cardinality.

If the cardinality is 1, then $S \cap B_i = \{(i, 0)\}$ so $j_2 = j_1$. Hence $g(j_1) = g(j_2)$, and since $S \cap B_{i'} = \{(i', 0)\}$, the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ . Similarly, if the cardinality is $m - 1$, then $S \cap B_i = \{B_i \setminus \{(i, 0)\}\}$ so $j_2 \neq j_1$. Hence $g(j_1) \neq g(j_2)$, and since $S \cap B_{i'} = \{B_{i'} \setminus \{(i', 0)\}\}$, the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ . Finally, if the cardinality is m , then $S \cap B_i = B_i$, and $S \cap B_{i'} = B_{i'}$, so the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ .

We have shown that $H \times S_m \leq \text{Aut}(\Gamma)$, as desired, and that $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$. It only remains to show that H is 2-closed. We have $H \times S_m$ admits \mathcal{B} , so by [10, Theorem 4.11], so does $(H \times S_m)^{(2)}$. Since $H \times S_m \leq \text{Aut}(\Gamma)$, we also have $(H \times S_m)^{(2)} \leq \text{Aut}(\Gamma)$ since $\text{Aut}(\Gamma)$ is 2-closed. By the definition of G , this means $(H \times S_m)^{(2)} \leq G$. By [3, Theorem 5.1] we have that $(H \times S_m)^{(2)} = H^{(2)} \times (S_m)^{(2)} = H^{(2)} \times S_m$, so $H^{(2)} \times S_m \leq G$. As H is projection of G into the first coordinate, we conclude that $H^{(2)} = H$ and H is 2-closed. This completes the first direction of the biconditional.

Now we assume that $\text{Aut}(\Gamma)$ contains a subgroup isomorphic to $H \times S_m$ with the canonical action, for some 2-closed group H with $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$.

Clearly the orbits of $\text{Stab}_{1 \times S_m}(0, 0)$ are transitive on $B_i \setminus \{(i, 0)\}$, and so the orbits of $\text{Stab}_{1 \times S_m}(0, 0)$ on B_i are $\{(i, 0)\}$ and $B_i \setminus \{(i, 0)\}$. Also $1 \times S_m \leq H \times S_m \leq \text{Aut}(\Gamma)$ implies $\text{Stab}_{1 \times S_m}(0, 0) \leq \text{Stab}_{H \times S_m}(0, 0) \leq \text{Stab}_{\text{Aut}(\Gamma)}(0, 0)$. Thus each $S \cap B_i$ is a union of some (possibly none) of these two orbits. Hence the only possibilities for each $S \cap B_i$ are $\emptyset, \{(i, 0)\}, B_i \setminus \{(i, 0)\}$ and B_i if $1 \leq i \leq k - 1$; and since $0 \notin S$, $S \cap B_0$ is either \emptyset or $B_0 \setminus \{(0, 0)\}$. \square

Notice that if Theorem 2.5(1) applies to $\text{Aut}(\Gamma)$ for some circulant digraph Γ , and some $G_i \cong S_m$ where $m \geq 4$, then $\text{Aut}(\Gamma) = H \times S_m$ for some H with $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$. Furthermore, since $\text{Aut}(\Gamma)$ is 2-closed and the 2-closure of a direct product is the direct product of the 2-closures of the

factors [3, Theorem 5.1], H is 2-closed, so the above lemma tells us that Γ is of deleted wreath type. We also observe that provided $m \geq 4$, a deleted wreath product type circulant digraph cannot be a normal circulant digraph.

Corollary 2.17 *There are at most $2^{n/m+1}$ graphs Γ and at most $2^{2n/m}$ digraphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$, where $m \geq 4$. Equivalently, there are at most $2^{2n/m}$ digraphs of deleted wreath type, and at most $2^{n/m+1}$ graphs of deleted wreath type, for any fixed $m \geq 4$ with $m \mid n$ and $\gcd(m, n/m) = 1$.*

PROOF. A consequence of Lemma 2.16 is that there are $2 \cdot 4^{n/m-1} < 4^{n/m} = 2^{2n/m}$ digraphs of order n whose automorphism group contains $K \times S_m$ for $m \geq 4$. Note that a digraph Γ with $\text{Aut}(\Gamma) = K \times S_m$, $m \geq 3$, is a graph if and only if K contains the map $\delta : \mathbb{Z}_{n/m} \rightarrow \mathbb{Z}_{n/m}$ given by $\delta(x) = -x$. Then $\delta(g + H) = (-g) + H$ where $H = \langle n/m \rangle$, and so if n/m is odd, there are at most $4^{n/(2m)} = 2^{n/m}$ graphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$. Even if n/m is even, only one nontrivial coset of $\langle n/m \rangle$ is fixed by δ , so there are at most $2 \cdot 4 \cdot 4^{(n/m-2)/2} = 2^{n/m+1}$ graphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$. \square

3 Normal Circulants

In this section our main focus is on determining whether or not almost all circulants that do not have automorphism groups as small as possible are normal circulants, as conjectured by the second author [4, Conjecture 1]. We show that this conjecture is false for circulant digraphs of order n where $n \equiv 2 \pmod{4}$ has a fixed number of distinct prime factors (Theorem 3.4). Additionally, we correct some oversights in [4, Theorem 3.5], and show that the conjecture is not true for circulant graphs of order p or p^2 , where p is a safe prime, or whose order is a power of 3 (Theorem 3.5). We also show that the conjecture is true for circulant digraphs of odd order n not divisible by 9 (Theorem 3.6), and for circulant graphs of order n if n is not a safe prime, the square of a safe prime, even, or a multiple of 9 (Theorem 3.7). We begin by showing that almost every circulant graph of order n has automorphism group as small as possible. We remark that Babai and Godsil [2, Theorem 5.3] have shown this to be true for abelian groups of order n , where $n \equiv 3 \pmod{4}$.

Let $\text{ACG}(n)$ be the set of all circulant graphs of order n , and $\text{Small}(n)$ be the set of all circulant graphs Γ of order n such that $\text{Aut}(\Gamma) = \langle \rho, \iota \rangle \cong D_n$, where $\iota(i) = -i$. Thus $\text{Small}(n)$ is the set of all circulant graphs whose automorphism groups are as small as possible.

Theorem 3.1 *Almost all circulant graphs are in $\text{Small}(n)$. That is,*

$$\lim_{n \rightarrow \infty} \frac{|\text{Small}(n)|}{|\text{ACG}(n)|} = 1.$$

PROOF. By Theorem 2.5 and Corollary 2.11, we have that a circulant graph of order n is either a generalized wreath circulant, or there exist G_1, \dots, G_r such that $\text{Aut}(\Gamma) = G_1 \times \dots \times G_r$, and for each G_i , either $G_i \cong S_{n_i}$, or G_i contains a normal regular cyclic group of order n_i , where $r \geq 1$, $\gcd(n_i, n_j) = 1$ for $i \neq j$, and $n = n_1 n_2 \dots n_r$. In Corollary 2.14, it is shown that there are at most $\log_2^2 n \cdot 2^{3n/8+1/2}$ generalized wreath circulant graphs of order n . Now, any circulant graph that is not a generalized wreath circulant graph of order n either has automorphism group which normalizes $\langle \rho \rangle$, or there is some G_i which is a symmetric group and $n_i \geq 4$. If G_i is a symmetric group and $n_i \geq 4$, then G_i contains a nontrivial automorphism of \mathbb{Z}_{n_i} . As we may assume n is arbitrarily large, we may assume that $n \neq 4$ or 6 . Then if $n_i = n$ or $n_i = n/2$, we may choose this automorphism so that it is not in $\langle \iota \rangle$. Otherwise (if $n_i < n/2$) there is some $n_j \geq 3$, and as $\gcd(n_i, n_j) = 1$ such an automorphism of \mathbb{Z}_{n_i} extends to an automorphism of \mathbb{Z}_n which is not contained in $\langle \iota \rangle$. In any case, we have an automorphism α of \mathbb{Z}_n contained in $\text{Aut}(\Gamma)$ but not in $\langle \iota \rangle$. Obviously, if $\langle \rho \rangle \triangleleft \text{Aut}(\Gamma)$, then either there exists an automorphism α of \mathbb{Z}_n contained in $\text{Aut}(\Gamma)$ but not in $\langle \iota \rangle$, or Γ is in $\text{Small}(n)$. Thus if Γ is not a generalized wreath circulant graph, then either Γ is in $\text{Small}(n)$ or there exists an automorphism α of \mathbb{Z}_n contained in $\text{Aut}(\Gamma)$ but not in $\langle \iota \rangle$.

Now observe that ι has at most two fixed points, and so has at most $(n-2)/2 + 2$ orbits. Let $\alpha \in \text{Aut}(\mathbb{Z}_n)$ be such that $\alpha \notin \langle \iota \rangle$. Observe that we may divide the orbits of $\langle \iota, \alpha \rangle$ into three types: singleton orbits, orbits of length 2, and orbits of length greater than 2. As $\langle \iota \rangle$ has at most 2 singleton orbits, $\langle \iota, \alpha \rangle$ has at most two singleton orbits, namely 0 and $n/2$. If $x \neq 0, n/2$, then x is contained in an orbit of $\langle \iota \rangle$ of length 2. If such an x is contained in an orbit of $\langle \iota, \alpha \rangle$ of length 2, then setting $\alpha(x) = ax$, $a \in \mathbb{Z}_n^*$, we have that $\{x, -x\} = \{ax, -ax\}$, in which case $x = ax$ and x is a fixed point of α or $x = -ax$ and x is a fixed point of $\iota\alpha$. If $x = ax$ set $\beta = \alpha$ and if $x = -ax$, set $\beta = \iota\alpha$. Then $\langle \iota, \alpha \rangle = \langle \iota, \beta \rangle$, and x is a fixed point of β . It is easy to see that the set of fixed points of β , say $H(\beta)$, forms a subgroup of \mathbb{Z}_n , and so $|H(\beta)| \leq n/2$. Thus $\langle \iota, \alpha \rangle$ has at at most $(n/2 - 1)/2$ orbits of length two, and so at most $(n/2 - 1)/2 + 2$ orbits of length one or two. Every remaining orbit of $\langle \iota, \alpha \rangle$ is a union of orbits of $\langle \iota \rangle$ of size 2, and so every remaining orbit of $\langle \iota, \alpha \rangle$ has length at least 4. Clearly, the number of orbits of $\langle \iota, \alpha \rangle$ is maximized if it has 2 orbits of length 1, $(n/2 - 1)/2$ orbits of length 2, and the remainder have length greater than 2. In this case, there will be at most $(n/2 - 1)/4 = n/8 - 1/4$ orbits of length greater than 2. We conclude that there are at most $3n/8 + 5/4$ orbits of $\langle \iota, \alpha \rangle$, and as S must be a union of orbits of $\langle \iota, \alpha \rangle$ not including $\{0\}$, there are at most $2^{3n/8+1/4}$ such circulant graphs for each $\alpha \in \text{Aut}(\mathbb{Z}_n)$, $\alpha \neq \iota$. As there are at most n (actually $\varphi(n)$ of course) automorphisms of \mathbb{Z}_n , there are at most $n \cdot 2^{3n/8+1/4}$ circulant

graphs that contain an automorphism of \mathbb{Z}_n other than ι .

We have shown that there are at most $n \cdot 2^{3n/8+1/4} + \log_2^2 n \cdot 2^{3n/8+1/2} < \sqrt{2}(n + \log_2^2 n)2^{3n/8}$ circulant graphs of order n that are not in $\text{Small}(n)$. As there are $2^{(n-2)/2+1} = 2^{n/2}$ circulant graphs of order n if n is even and $2^{(n-1)/2}$ circulant graphs of order n if n is odd,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{|\text{Small}(n)|}{|\text{ACG}(n)|} &\geq 1 - \lim_{n \rightarrow \infty} \frac{\sqrt{2}(n + \log_2^2 n)2^{3n/8}}{2^{(n-1)/2}} \\ &= 1 - \lim_{n \rightarrow \infty} \frac{2(n + \log_2^2 n)}{2^{n/8}} = 1. \end{aligned}$$

□

The above theorem clearly shows that almost all circulant graphs are normal. In 2010, the second author proposed the following conjecture for Cayley (di)graphs (not necessarily circulant) whose automorphism group is not as small as possible [4, Conjecture 1].

Conjecture 3.2 *Almost every Cayley (di)graph whose automorphism group is not as small as possible is a normal Cayley (di)graph.*

It is difficult to determine the automorphism group of a (di)graph, so the main way to obtain examples of vertex-transitive graphs is to construct them. An obvious construction is that of a Cayley (di)graph, and the conjecture of Imrich, Lovász, Babai, and Godsil says that when performing this construction, additional automorphisms are almost never obtained. The obvious way of constructing a Cayley (di)graph of G that does not have automorphism group as small as possible is to choose an automorphism α of G and make the connection set a union of orbits of α . The above conjecture in some sense says that this construction almost never yields additional automorphisms other than the ones given by the construction.

Throughout the remainder of this paper, all circulant digraphs of order n whose automorphism groups are of generalized wreath, deleted wreath, and strictly deleted wreath types will be denoted by $\text{GW}(n)$, $\text{DW}(n)$, and $\text{SDW}(n)$ respectively. The corresponding sets of all graphs whose automorphism groups are of generalized wreath and deleted wreath type will be denoted by $\text{GWG}(n)$ and $\text{DWG}(n)$, respectively. Also, the sets of all digraphs that are circulants, DRR circulants, normal circulants, and non-normal circulants of order n will be denoted as $\text{ACD}(n)$, $\text{DRR}(n)$, $\text{Nor}(n)$ and $\text{NonNor}(n)$, respectively. The corresponding sets of all graphs that are circulants, normal circulants, and nonnormal circulants, will be denoted by $\text{ACG}(n)$, $\text{NorG}(n)$, and $\text{NonNorG}(n)$, respectively.

The following lemma will prove useful in determining how many circulant (di)graphs are not normal.

Lemma 3.3 *A circulant digraph Γ of composite order n that is a (K, H) -generalized wreath circulant digraph is not normal if n is not divisible by 4.*

PROOF. As usual, let $\rho : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $\rho(i) = i + 1 \pmod{n}$. In this proof, we will use the notation $N(n)$ for the normaliser of $\langle \rho \rangle$; that is, the group of permutations of \mathbb{Z}_n given by $\{x \rightarrow ax + b : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$. We will show that if a (K, H) -generalized wreath circulant is normal, then $4 \mid n$.

We may assume without loss of generality that K is of prime order p . Let \mathcal{B} be the complete block system of $\langle \rho \rangle$ formed by the orbits of $\langle \rho^m \rangle$, where $|H| = n/m$. Then $\rho^{n/p}|_B \in \text{Aut}(\Gamma)$ for every $B \in \mathcal{B}$. Set $G = \langle \rho, \rho^{n/p}|_B : B \in \mathcal{B} \rangle$, and let \mathcal{C} be the complete block system of G formed by the orbits of $\langle \rho^{n/p} \rangle$, so that $\text{fix}_G(\mathcal{C}) = \langle \rho^{n/p}|_B : B \in \mathcal{B} \rangle$, and has order $p^{n/m}$. Then \mathcal{C} is also a complete block system of $N(n)$. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime power decomposition of n . As $N(n) = \prod_{i=1}^r N(p_i^{a_i})$, we see that a Sylow p -subgroup of $\text{fix}_{N(n)}(\mathcal{C})$ is a Sylow p -subgroup of $1_{S_{n/p^a}} \times N(p^a)$, where $p = p_j$ and $a = a_j$ for some j . Let \mathcal{E} be the complete block system of $N(p^a)$ consisting of blocks of size p . Then a Sylow p -subgroup of $\text{fix}_{N(p^a)}(\mathcal{E})$ has order at most p^2 as a Sylow p -subgroup of $N(p^a)$ is metacyclic. If Γ is a normal circulant digraph, then $\langle \rho \rangle \triangleleft G$ since $G \leq \text{Aut}(\Gamma)$, so $G \leq N(n)$. This implies that a Sylow p -subgroup of $\text{fix}_G(\mathcal{C})$ has order at most p^2 , and so $p^{n/m} \leq p^2$. Since $H > 1$ we have $n > m$, so this forces $n = 2m$, and \mathcal{B} consists of 2 blocks. Finally, let $\delta = \rho^{n/p}|_B$, where $B \in \mathcal{B}$ with $0 \in B$. If Γ is a normal circulant digraph, then $\gamma = \rho^{-1} \delta^{-1} \rho \delta \in \langle \rho \rangle$, and straightforward computations will show that $\gamma(i) = i + n/p$ if i is even, while $\gamma(i) = i - n/p$ if i is odd. As $\gamma \in \langle \rho \rangle$, we must have that $n/p \equiv -n/p \pmod{n}$, and so $2n/p \equiv 0 \pmod{n}$. This then implies that $p = 2$ and so $4 \mid n$ as required. \square

We first show that Conjecture 3.2 is false for circulant digraphs of order n , where $n \equiv 2 \pmod{4}$ has a fixed number of distinct prime factors.

Theorem 3.4 *Let $n = 2p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where each p_i is a distinct odd prime and r is fixed. Then*

$$\lim_{n \rightarrow \infty, r \text{ fixed}} \frac{|\text{NonNor}(n)|}{|\text{Nor}(n) \setminus \text{DRR}(n)|} \geq \frac{1}{4(2^r - 1)}.$$

PROOF. By Lemma 3.3, we have $|\text{NonNor}(n)| \geq |\text{GW}(n)|$. We claim that $|\text{GW}(n)| \geq 2^{n/2 + n/(2p) - 1}$, where p is the smallest nontrivial divisor of $n/2$. To see this, we construct this number of distinct generalized circulant digraphs of order n , as follows: \mathcal{B} will be the block system formed by the orbits (cosets) of $\langle n/2 \rangle$, and \mathcal{C} the block system formed by the orbits (cosets) of $\langle p \rangle$. Since there are n/p elements in each block of \mathcal{C} , there are $2^{n/p-1}$ choices for $S \cap C_0$, where C_0 is the block of \mathcal{C} that contains 0. Since there are $n/2 - n/(2p)$ orbits (cosets) of $\langle n/2 \rangle$ that are not in C_0 , there are $2^{n/2 - n/(2p)}$ choices for $S - C_0$ that create a generalized circulant digraph with this choice of \mathcal{B} and \mathcal{C} . These $2^{n/p + n/2 - n/(2p) - 1} = 2^{n/2 + n/(2p) - 1}$ generalized circulant digraphs are all distinct (though

not necessarily nonisomorphic), so there are indeed at least this many distinct generalized circulant digraphs of order n .

Let $S(n)$ be the set of all circulant digraphs of order n whose automorphism group contains a nontrivial automorphism of \mathbb{Z}_n . Clearly then $|S(n)| \geq |\text{Nor}(n) \setminus \text{DRR}(n)|$. We now seek an upper bound on $|S(n)|$. Observe that if Γ is a circulant digraph whose automorphism group contains a nontrivial automorphism of \mathbb{Z}_n , then $\text{Aut}(\Gamma)$ contains a nontrivial automorphism of \mathbb{Z}_n of prime order.

Let $a \in \mathbb{Z}_n^*$ have prime order ℓ , $a \neq 1$, and let $\alpha : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be defined by $\alpha(i) = ai$. We first consider the case that α has a fixed point other than 0. If α fixes a point i , so that $ai \equiv i \pmod{n}$, then $(a - 1)i \equiv 0 \pmod{n}$. If $\gcd(i, n) = 1$, then $a = 1$ and α is the identity, a contradiction. Otherwise, $\gcd(i, n) = m$, for some non-trivial integer m , which clearly implies $i \in \langle m \rangle$. In order for α to be an automorphism, $a = sn/m + 1$ for some $0 < s < m$ must be a unit, i.e., $\gcd(n, sn/m + 1) = 1$. Note that $m \neq 2$ for our choice of n , since if $m = 2$ then $s = 1$, but $\gcd(n, n/2 + 1) \geq 2$. So m must be a divisor of n that is greater than 2 and less than n . Now, α fixes n/m points $\{0, m, \dots, (n/m - 1)m\}$, and since the order of α is prime (ℓ), every non-singleton orbit of α has length ℓ . So α has $n(1 - 1/m)/\ell$ orbits of length ℓ , and $n/m + n/\ell - n/(m\ell)$ orbits in total. It will be necessary to separate out the cases where $\ell = 2$ and $\ell = 3$. If $\ell = 2$ then $1/m + 1/\ell - 1/(m\ell) = 1/m + 1/2 - 1/(2m) = 1/2 + 1/(2m) \leq (p + 1)/(2p)$ since $m \geq p$ (p is still the smallest nontrivial divisor of $n/2$), so if α has order 2 then α has at most $(p + 1)n/(2p)$ orbits. If $\ell = 3$ then $1/m + 1/\ell - 1/(m\ell) = 1/m + 1/3 - 1/(3m) = 1/3 + 2/(3m) \leq (p + 2)/(3p)$ since $m \geq p$, so if α has order 3 then α has at most $(p + 2)n/(3p)$ orbits. And if $\ell \geq 5$ then $1/m + 1/\ell - 1/(m\ell) \leq 1/m + 1/5 - 1/(5m) = 1/5 + 4/(5m) \leq (m + 4)/(5m) \leq 7/15$ since $m \geq 3$, so if α has order greater than 3 then α has at most $7n/15$ orbits.

Finally, notice that if α fixes only 0, it will have 1 fixed point and $n - 1$ points that are not fixed. If α has order 2 then its orbits are all of length 1 or 2, and since $n - 1$ is odd, it cannot be partitioned into orbits of length 2. So an element of order 2 must have some fixed point other than 0. Hence if α fixes only 0, it must have order at least 3, so each non-singleton orbit must have length at least 3. Hence α has at most $\lfloor (n - 1)/3 \rfloor < n/3$ orbits other than $\{0\}$.

From these bounds on the number of orbits of α , we can deduce bounds on the number of normal circulant digraphs of order n that admit α as an automorphism. We now want to sum the upper bounds on the numbers of normal circulant digraphs of order n that admit α , over all automorphisms α of \mathbb{Z}_n that have prime order. In order to do so, we split the set T of all elements of \mathbb{Z}_n^* that have prime order, into disjoint subsets: U (consisting of all elements of order 2 that have fixed points); V (consisting of all elements of order 3 that have fixed points); W (consisting of all elements of order 5 or greater that have fixed points) and X (consisting of all elements that have

no fixed points other than 0). Notice that $|T| \leq |\mathbb{Z}_n^*| \leq \phi(n) < n$, so the order of each set is less than n . We will need slightly better estimates for $|U|$ and $|V|$; but first, observe that

$$|S(n)| \leq \sum_{\alpha \in U} 2^{(p+1)n/(2p)} + \sum_{\alpha \in V} 2^{(p+2)n/(3p)} + \sum_{\alpha \in W} 2^{7n/15} + \sum_{\alpha \in X} 2^{n/3}.$$

Notice that $\mathbb{Z}_n^* = \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ and each $\mathbb{Z}_{p_i}^*$ is cyclic, so contains a unique element of order 2, and at most one element of order 3. Any element of order 2 in \mathbb{Z}_n^* must be a product of elements of order 1 or 2 from the $\mathbb{Z}_{p_i}^*$, at least one of which must have order 2. So there are $2^r - 1$ elements of order 2 in \mathbb{Z}_n^* . Similarly, there are at most $2^r - 1$ elements of order 3 in \mathbb{Z}_n^* . Thus the above sum yields

$$|S(n)| \leq (2^r - 1)2^{(p+1)n/(2p)} + (2^r - 1)2^{(p+2)n/(3p)} + n2^{7n/15} + n2^{n/3}.$$

Since $p > 1$ we have $(p+2)/(3p) < (p+1)/(2p)$, so

$$|S(n)| \leq (2^r - 1)2^{(p+1)n/(2p)+1} + n2^{7n/15} + n2^{n/3}.$$

Now

$$\begin{aligned} \lim_{n \rightarrow \infty, r \text{ fixed}} \frac{|\text{NonNor}(n)|}{|\text{Nor}(n) \setminus \text{DRR}(n)|} &\geq \lim_{n \rightarrow \infty, r \text{ fixed}} \frac{2^{n/2+n/(2p)-1}}{|S(n)|} \\ &\geq \lim_{n \rightarrow \infty, r \text{ fixed}} \frac{2^{n/2+n/(2p)-1}}{(2^r - 1)2^{(p+1)n/(2p)+1} + n2^{7n/15} + n2^{n/3}} \\ &= \lim_{n \rightarrow \infty, r \text{ fixed}} \frac{2^{-1}}{2(2^r - 1) + n2^{-n/30-n/(2p)} + n2^{-n/6-n/(2p)}} \\ &= \frac{1}{4(2^r - 1)}. \end{aligned}$$

□

A **safe prime** is a prime number $p = 2q + 1$, where q is also prime.

We now show that it is not true that almost all circulant graphs of order p or p^2 , where p is a safe prime, or of order 3^k , are normal. This shows that [4, Theorem 3.5] is not correct. We provide a correct statement of [4, Theorem 3.5] as well as point out explicitly where “gaps” occur in the proof. As a consequence, much of the following result is essentially the same as the proof of [4, Theorem 3.5]. The entire argument is included for completeness.

Theorem 3.5 *Let $S = \{p, p^2 : p \text{ is a safe prime}\} \cup \{3^k : k \in \mathbb{N}\}$, T the set of all powers of odd primes, and $R = T \setminus S$. Then*

$$\lim_{n \in R, n \rightarrow \infty} \frac{|\text{NonNorG}(n)|}{|\text{ACG}(n) \setminus \text{Small}(n)|} = 0.$$

Additionally, if $n \in S$, then more than one fifth of all elements of $\text{ACG}(n) \setminus \text{Small}(n)$ are in $\text{NonNorG}(n)$.

PROOF. Let $n = p^k$, where p is an odd prime.

First suppose that $k = 1$. If p is a safe prime, then \mathbb{Z}_p^* is cyclic of order $2q$, so every element has order 2, q , or $2q$. Since a circulant graph must have ι (multiplication by -1) in its automorphism group, if a circulant graph of order p is not in $\text{Small}(p)$ then it must have an automorphism α of order q or $2q$ from \mathbb{Z}_p^* in its automorphism group. Since the orbit of length q that contains 1 in \mathbb{Z}_p^* does not contain -1 , the orbits of $\langle \alpha, \iota \rangle$ have length 1 (the orbit of 0) and $2q = p - 1$ (everything else). So the graph must be either K_p or its complement. Both of these are non-normal circulants (with automorphism group S_p), so in this case all elements of $\text{ACG}(n) \setminus \text{Small}(n)$ are in $\text{NonNorG}(n)$. (The proof of [4, Theorem 3.5] overlooks this case.)

Now if p is not a safe prime, then $(p - 1)/2$ is a composite number, say $(p - 1)/2 = rs$ where $1 < r \leq s < (p - 1)/2$. As p tends to infinity, so does s . Now, \mathbb{Z}_p^* is cyclic of order $p - 1$, so has an element, α say, of order $2r$. The action of α on the elements of \mathbb{Z}_p will have $s + 1$ orbits (the cosets of $\langle 2r \rangle$ in \mathbb{Z}_p^* , together with 0). Since the order of α is even, $-1 \in \langle \alpha \rangle$, so if we let S be any union of these orbits, the circulant digraph on \mathbb{Z}_p with connection set S will be a graph, and since $|\alpha| > 2$, this graph will not be in $\text{Small}(p)$. Hence $|\text{ACG}(p) \setminus \text{Small}(p)| \geq 2^{s+1} > 2\sqrt{(p-1)/2}$. Meanwhile, if $\text{Aut}(\Gamma) \not\leq \text{AGL}(1, p)$ then $\text{Aut}(\Gamma) = S_p$ by [1], and so there are only two non-normal Cayley graphs on \mathbb{Z}_p , namely K_p or its complement. Clearly $2/(2\sqrt{(p-1)/2})$ tends to 0 as p tends to infinity.

Now let $k \geq 2$. Through the rest of this proof, let $\alpha : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be defined by $\alpha(i) = (p^{k-1} + 1)i$. Using the binomial theorem, it is easy to see that $|\alpha| = p$. Furthermore, α fixes every element of $\langle p \rangle$, and fixes setwise every coset of $\langle p^{k-1} \rangle$. Since α has order p and α does not fix any element of any coset of $\langle p^{k-1} \rangle$ that is not in $\langle p \rangle$, it follows that the orbits of α on each coset of $\langle p^{k-1} \rangle$ that is not in $\langle p \rangle$ have length p , so if $\alpha \in \text{Aut}(\Gamma)$ for some circulant graph Γ of order n , then Γ is a $(\langle p^{k-1} \rangle, \langle p \rangle)$ -generalized wreath circulant digraph, and in fact by Lemma 3.3, Γ is not normal. Conversely, if Γ is a non-normal circulant graph of order n , then by Theorem 2.5, the automorphism group of a circulant graph of order n either falls into category (1) with a single factor in the direct product (since $n = p^k$ does not permit coprime factors) and consequently since it is non-normal, is complete (or empty), or category (2) so by Corollary 2.11 is a generalized wreath circulant. Since complete and empty graphs are generalized wreath circulants, Γ must be a generalized wreath circulant graph. It is straightforward to verify using the definition of a generalized wreath circulant, that $\alpha \in \text{Aut}(\Gamma)$. Notice also that if p divides the order of some element b of \mathbb{Z}_n^* such that multiplication by b is in $\text{Aut}(\Gamma)$, then $\alpha \in \text{Aut}(\Gamma)$, since \mathbb{Z}_n^* is cyclic of order $(p - 1)p^{k-1}$ so $p^{k-1} + 1$ generates the unique subgroup of order p in \mathbb{Z}_n^* .

Now we calculate $|\text{NonNorG}(n)|$. As noted in the previous paragraph, if $\Gamma \in \text{NonNorG}(n)$ then $\alpha \in \text{Aut}(\Gamma)$, and the orbits of α all have length 1 or length p . Now since multiplication is commutative, if ι is as usual the automorphism given by multiplication by -1 , then ι will have a

well-defined action on the orbits of $\langle \alpha \rangle$, and since $|\alpha| = p$ is odd, $\iota \notin \langle \alpha \rangle$, so ι will exchange pairs of orbits of $\langle \alpha \rangle$, except the orbit $\{0\}$. Consequently, $\langle \alpha, \iota \rangle$ will have one orbit of length 1 ($\{0\}$); $(p^{k-1} - 1)/2$ orbits of length 2 (whose union is $\langle p \rangle \setminus \{0\}$); and $(p^k - p^{k-1})/(2p)$ orbits of length $2p$ (everything else). So $\langle \alpha, \iota \rangle$ has a total of exactly $p^{k-1} + (1 - p^{k-2})/2$ orbits. Since we have shown that the non-normal circulant graphs of order p^k are precisely the graphs that have $\langle \alpha, \iota \rangle$ in their automorphism group, there are exactly $2^{p^{k-1} + (1 - p^{k-2})/2}$ non-normal circulant graphs of order p^k .

Now we find a lower bound for $|\text{ACG}(n) \setminus \text{Small}(n)|$ when $n \in R$ and $k > 2$. Since p is an odd prime, $\mathbb{Z}_{p^k}^*$ is cyclic of order $(p - 1)p^{k-1}$. Since $p > 3$, let b be an element of order $p - 1$ in $\mathbb{Z}_{p^k}^*$, and define $\beta : \mathbb{Z}_{p^k} \rightarrow \mathbb{Z}_{p^k}$ by $\beta(x) = bx$. Note that $\iota \in \langle \beta \rangle$ since β has even order, and $\beta \neq \iota$ since $p > 3$ (the proof of [4, Theorem 3.5] overlooks the fact that $\beta = \iota$ when $p = 3$). Clearly, β fixes 0, and since the order of β is $p - 1$, every other orbit of β has length at most $p - 1$, so β has at least $1 + (p^k - 1)/(p - 1)$ orbits. Thus there are at least $2^{1 + (p^k - 1)/(p - 1)}$ circulant graphs of order p^k whose automorphism group contains β , and so there are at least $2^{1 + (p^k - 1)/(p - 1)}$ circulant graphs of order p^k that are not in $\text{Small}(p^k)$, $p > 3$. Note that as $k \geq 2$, $(p^k - 1)/(p - 1) \neq 1$. Then

$$\begin{aligned} \lim_{p^k \rightarrow \infty} \frac{|\text{NonNorG}(p^k)|}{|\text{ACG}(p^k) \setminus \text{Small}(p^k)|} &\leq \lim_{p \rightarrow \infty} \frac{2^{p^{k-1} + (1 - p^{k-2})/2}}{2^{1 + (p^k - 1)/(p - 1)}} \\ &= \lim_{p^k \rightarrow \infty} \frac{1}{2^{(3p^{k-2} + 1)/2 + \sum_{i=0}^{k-3} p^i}}. \end{aligned}$$

Thus as $k \geq 3$, the result follows. (The proof of [4, Theorem 3.5] concludes the above limit is 1 in all cases – hence the gap in that theorem when $k = 2$).

We now consider the case $p = 3$. We have $\mathbb{Z}_{3^k}^*$ is cyclic of order $2 \cdot 3^{k-1}$. For a circulant graph Γ of order 3^k to be normal but not in $\text{Small}(3^k)$, there must be an automorphism of Γ that corresponds to multiplying by some element, b say, of $\mathbb{Z}_{3^k}^*$. As noted previously (in the paragraph about α), if $|b|$ is divisible by 3, then $\alpha \in \text{Aut}(\Gamma)$ and hence Γ is not normal. But the only possible order for b that is not divisible by 3 is 2, which corresponds to $b = -1$. This shows that every circulant graph of order 3^k that is normal, is in $\text{Small}(3^k)$, so in other words, every element of $\text{ACG}(3^k) \setminus \text{Small}(3^k)$ is in $\text{NonNorG}(3^k)$.

For the remainder of the proof we suppose that $k = 2$ and $p > 3$. Substituting $k = 2$ into our formula for $|\text{NonNorG}(n)|$, we conclude that $|\text{NonNorG}(p^2)| = 2^p$.

If p is a safe prime, $p = 2q + 1$ with q prime, then $\langle \alpha \rangle$ is the unique subgroup of order p in $\mathbb{Z}_{p^2}^*$, so any subgroup of $\mathbb{Z}_{p^2}^*$ that contains -1 but does not contain $p + 1$, must have even order not a multiple of p . Since $\mathbb{Z}_{p^2}^*$ is cyclic of order $p(p - 1) = 2pq$, the group of order $2q$ is the only such subgroup. Call this group B . Then if Γ is normal and does not have automorphism group as small as possible, then $\text{Aut}(\Gamma) = B \cdot (\mathbb{Z}_{p^2})_L$. Now, B fixes 0 and since B has order $2q$ and is cyclic, the other orbits of B all have length precisely $2q$ (it is not hard to show that the only elements of

$\mathbb{Z}_{p^2}^*$ that fix anything but 0 are 1 and the elements of order p ; this forces the orbit lengths of B to be the order of B), so there are $1 + (p^2 - 1)/2q = 2 + p$ orbits of B , and hence fewer than 2^{2+p} normal circulant graphs of order p^2 that are not in $\text{Small}(p^2)$ (the “fewer than” is due to the fact that some of these graphs are not normal, for example K_{p^2}). Hence the proportion of non-normal circulant graphs of order p^2 in the set of all circulant graphs of order p^2 that are not in $\text{Small}(p^2)$ is more than $2^p/(2^p + 2^{p+2}) = 1/5$, as claimed.

Suppose now that p is not a safe prime. Then there exists $b \in \mathbb{Z}_{p^2}^*$ of order $p - 1$. Since p is not a safe prime, there exists $1 < s \leq r < (p - 1)/2$ such that $rs = (p - 1)/2$. Let β be the map defined by multiplication by b . As every non-singleton orbit of $\langle \beta \rangle$ has length $p - 1$ (as shown for the orbits of B in the preceding paragraph), every nonsingleton orbit of $\langle \beta^r \rangle$ has length $(p - 1)/r$. Then β^r has $r(p + 1)$ orbits not including $\{0\}$ and since $|b^r| = 2s > 2$, $\beta^r \neq \iota$. We conclude that there are at least $2^{r(p+1)}$ graphs of order p^2 not contained in $\text{Small}(p^2)$. As there are 2^p non-normal circulant graphs of order p^2 and $r > 1$,

$$\lim_{p^2 \rightarrow \infty} \frac{|\text{NonNorG}(p^2)|}{|\text{ACG}(p^2) \setminus \text{Small}(p^2)|} \leq \lim_{p \rightarrow \infty} \frac{2^p}{2^{r(p+1)}} = 0.$$

Since $r \geq \sqrt{(p - 1)/2}$, we may now conclude that

$$\lim_{n \in R, n \rightarrow \infty} \frac{|\text{NonNorG}(n)|}{|\text{ACG}(n) \setminus \text{Small}(n)|} = 0.$$

□

We now verify that Conjecture 3.2 does hold for circulant digraphs of order n , and also for circulant graphs of order n , for large families of integers.

Theorem 3.6 *Let n be any odd integer such that $9 \nmid n$. Then almost all circulant digraphs of order n that are not DRR's are normal circulant digraphs.*

PROOF. It suffices to show that

$$\lim_{n \rightarrow \infty} \frac{|\text{NonNor}(n)|}{|\text{ACD}(n) \setminus \text{DRR}(n)|} = 0 \tag{1}$$

Given any circulant digraph Γ of order n , $\text{Aut}(\Gamma)$ falls into either category (1) or (2) of Theorem 2.5. By Corollary 2.11, if $\text{Aut}(\Gamma)$ falls into category (2), then Γ is a generalized wreath circulant digraph. By Lemma 2.16, if Γ falls into category (1) and is not normal, then Γ is of deleted wreath type. Hence $|\text{ACD}(n)| \leq |\text{Nor}(n)| + |\text{DW}(n)| + |\text{GW}(n)|$, which immediately implies $|\text{NonNor}(n)| \leq |\text{DW}(n)| + |\text{GW}(n)|$. Also, a lower bound for $|\text{ACD}(n) \setminus \text{DRR}(n)|$ is the number of circulant graphs of order n , which is $2^{(n-1)/2}$. Thus to establish (1), it suffices to show that

$$\lim_{n \rightarrow \infty} \frac{|\text{DW}(n)| + |\text{GW}(n)|}{2^{(n-1)/2}} = 0.$$

Also note that an upper bound for $|\text{GW}(n)|$ is given by Corollary 2.13. We now consider an upper bound for $|\text{DW}(n)|$.

Since n is odd, we have $2n/m \leq 2n/5$ for every nontrivial divisor $m \geq 4$ of n (of course, in this context $m \geq 5$). Also, n is an upper bound on the number of nontrivial divisors of n . By Corollary 2.17,

$$\lim_{n \rightarrow \infty} \frac{|\text{DW}(n)|}{2^{(n-1)/2}} \leq \lim_{n \rightarrow \infty} \frac{\sum_{m|n, m \geq 4} 2^{2n/m}}{2^{(n-1)/2}} \leq \lim_{n \rightarrow \infty} \frac{n \cdot 2^{2n/5}}{2^{(n-1)/2}} = 0.$$

It thus suffices to show that $\lim_{n \rightarrow \infty} |\text{GW}(n)|/2^{(n-1)/2} = 0$.

By Corollary 2.13, we have $|\text{GW}(n)| \leq \log_2^2 n \cdot 2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q . Since n is odd we have $q \geq 3$, and since $9 \nmid n$ we have $p \geq 5$. If $q \geq 5$ then $1/p + 1/q - 1/(pq) < 1/p + 1/q \leq 2/5$, while if $q = 3$ then $1/p + 1/q - 1/(pq) = 2/(3p) + 1/3 \leq 7/15$, so we always have $1/p + 1/q - 1/(pq) \leq 7/15$. Thus

$$\lim_{n \rightarrow \infty} \frac{|\text{GW}(n)|}{2^{(n-1)/2}} \leq \lim_{n \rightarrow \infty} \frac{\log_2^2 n \cdot 2^{n(1/p+1/q-1/(pq))-1}}{2^{(n-1)/2}} \leq \lim_{n \rightarrow \infty} \frac{\log_2^2 n \cdot 2^{7n/15}}{2^{(n+1)/2}} = \lim_{n \rightarrow \infty} \frac{\log_2^2 n}{\sqrt{2} \cdot 2^{n/30}} = 0$$

Note that if $9|n$ then $p = q = 3$ and so the immediately preceding limit does not go to 0. \square

Theorem 3.7 *Let n be any odd integer such that $9 \nmid n$, and n is not a safe prime or the square of a safe prime. Then almost all circulant graphs of order n that do not have automorphism group as small as possible are normal circulant graphs.*

PROOF. We need to show that

$$\lim_{n \rightarrow \infty, n \notin S} \frac{|\text{NonNorG}(n)|}{|\text{ACG}(n) \setminus \text{Small}(n)|} = 0,$$

where $S = \{p, p^2 : p \text{ is a safe prime}\} \cup \{n : 9 \mid n\} \cup \{n : 2 \mid n\}$. This is true if n is a prime power by Theorem 3.5. Henceforth, we assume that n is not a prime power. We may thus assume that there is a proper divisor m of n such that $\gcd(m, n/m) = 1$. We assume without loss of generality that $n/m > m$, and regard \mathbb{Z}_n as $\mathbb{Z}_{n/m} \times \mathbb{Z}_m$ in the natural way.

Given any circulant graph Γ of order n , $\text{Aut}(\Gamma)$ falls into either category (1) or (2) of Theorem 2.5. By Corollary 2.11, if $\text{Aut}(\Gamma)$ falls into category (2), then Γ is a generalized wreath circulant graph. By Lemma 2.16, if Γ falls into category (1) and is not normal, then Γ is of deleted wreath type. Hence $|\text{ACG}(n)| \leq |\text{NorG}(n)| + |\text{DWG}(n)| + |\text{GWG}(n)|$, which immediately implies $|\text{NonNorG}(n)| \leq |\text{DWG}(n)| + |\text{GWG}(n)|$.

First we find a lower bound for $|\text{ACG}(n) \setminus \text{Small}(n)|$. Let $\Gamma \in \text{ACG}(n)$ such that $\alpha \in \text{Aut}(\Gamma)$ where $\alpha(i, j) = (i, -j)$ for all $(i, j) \in \mathbb{Z}_{n/m} \times \mathbb{Z}_m$. Obviously $\alpha \notin \langle \rho, \iota \rangle$ which implies $\Gamma \notin \text{Small}(n)$.

Clearly if $\alpha \in \text{Aut}(\Gamma)$, then $\langle \alpha, \iota \rangle \leq \text{Aut}(\Gamma)$. It is straightforward to check that the orbits of $\langle \alpha, \iota \rangle$ are $\{(0, 0)\}$, $\{(i, 0), (-i, 0)\}$, $\{(0, j), (0, -j)\}$, and $\{(i, j), (-i, j), (i, -j), (-i, -j)\}$, where $i \in \mathbb{Z}_{n/m} \setminus \{0\}$ and $j \in \mathbb{Z}_m \setminus \{0\}$. We conclude that $\langle \alpha, \iota \rangle$ has

$$1 + \frac{n/m - 1}{2} + \frac{m - 1}{2} + \frac{n - n/m - m + 1}{4} = \frac{n + n/m + m + 1}{4} > \frac{n}{4}$$

orbits. Hence there are at least $2^{n/4}$ circulant graphs of order n that are not in $\text{Small}(n)$, and we will be done if we can show that

$$\lim_{n \rightarrow \infty, n \notin S} \frac{|\text{DWG}(n)| + |\text{GWG}(n)|}{2^{n/4}} = 0.$$

By Corollary 2.17 there are at most $\sum_{m|n, m \geq 4} 2^{n/m+1}$ graphs in $\text{DWG}(n)$. Since n is odd, if $m \geq 4$ and $m | n$ then $m \geq 5$, so $n/m \leq n/5$, and $\sum_{m|n, m \geq 4} 2^{n/m+1} \leq n 2^{n/5+1}$. Then

$$\lim_{n \rightarrow \infty, n \notin S} \frac{|\text{DWG}(n)|}{|\text{ACG}(n) \setminus \text{Small}(n)|} \leq \frac{2n 2^{n/5}}{2^{n/4}} = \frac{2n}{2^{n/20}} = 0.$$

It thus suffices to show that $\lim_{n \rightarrow \infty, n \notin S} |\text{GWG}(n)|/2^{n/4} = 0$.

By Corollary 2.14 there are at most $(\log_2^2 n) 2^{n(p+q-1)/(2pq)+1/2}$ generalized wreath circulant graphs of order n , where p is the smallest divisor of n and q is the smallest divisor of n/p . As in the proof of Theorem 3.6, it is straightforward to show that since n is odd and not divisible by 9, $(p+q-1)/(pq) \leq 7/15$. Hence

$$\lim_{n \rightarrow \infty, n \notin S} \frac{|\text{GWG}(n)|}{2^{n/4}} \leq \lim_{n \rightarrow \infty, n \notin S} \frac{(\log_2^2 n) 2^{7n/30+1/2}}{2^{n/4}} = \frac{\sqrt{2} \log_2^2 n}{2^{n/60}} = 0.$$

□

4 Non-normal Circulants

By Theorem 2.5, a circulant (di)graph that is not normal is of either generalized wreath or deleted wreath type. In this section we will consider whether or not almost all non-normal circulant (di)graphs of order n are in either one of these two classes. The short answer is “No” and is given by the following result.

Theorem 4.1 *Let Γ be a circulant digraph of order pq , where p and q are primes and $p, q \geq 5$. Then*

1. *if $q \neq p$ then*

$$\frac{|\text{GW}(pq)|}{|\text{SDW}(pq)|} = \frac{2^{p+q-1} - 2}{2^{2p-1} + 2^{2q-1} - 2^p - 2^q - 2},$$

2. if p is fixed, then $\lim_{q \rightarrow \infty} |\text{GW}(pq)|/|\text{SDW}(pq)| = 0$,
3. if $q = p + c$ for some constant $c \geq 2$, then $\lim_{p \rightarrow \infty} |\text{GW}(pq)|/|\text{SDW}(pq)| = 2^c/(1 + 2^{2c})$
4. if $q = p$ then all non-normal circulants are generalized wreath products.

PROOF. (1): We require exact counts of $|\text{GW}(pq)|$ and of $|\text{SDW}(pq)|$. First, the generalized wreath products. When $n = pq$ a generalized wreath product will actually be a wreath product. For a wreath product digraph with p blocks of size q , there are $q - 1$ possible elements of $S \cap \langle p \rangle$, and $p - 1$ choices for the cosets of $\langle p \rangle$ to be in S . Hence there are 2^{p+q-2} wreath product circulant digraphs with p blocks of size q . Similarly, there are 2^{q+p-2} wreath product circulant digraphs with q blocks of size p . The only digraphs that have both of these properties are K_{pq} and its complement, each of which has been counted twice, so $|\text{GW}(pq)| = 2 \cdot 2^{p+q-2} - 2 = 2^{p+q-1} - 2$.

Now we count strictly deleted wreath products. As mentioned in the first sentence of the proof of Corollary 2.17, there are precisely $2 \cdot 4^{p-1}$ digraphs whose automorphism group contains $K \times S_q$, and $2 \cdot 4^{q-1}$ digraphs whose automorphism group contains $K' \times S_p$. Of the first set, $2 \cdot 2^{p-1}$ are wreath products (those in which $S \cap (rq + \langle p \rangle)$ is chosen from $\{\emptyset, rq + \langle p \rangle\}$, for every $1 \leq r \leq p - 1$). Similarly, of the second set, $2 \cdot 2^{q-1}$ are wreath products (those in which $S \cap (rp + \langle q \rangle)$ is chosen from $\{\emptyset, rp + \langle q \rangle\}$, for every $1 \leq r \leq q - 1$). Finally, notice that if a digraph is counted in both the first and second sets then its automorphism group must contain $S_q \times S_p$. Consequently, the number of elements in $S \cap (rp + \langle q \rangle)$ is constant over r , as is the number of elements in $S \cap (rq + \langle p \rangle)$. Since we have already eliminated wreath products from our count, the first number must be 1 or $p - 1$, and the second must be 1 or $q - 1$. Furthermore, if the first number is 1 then we have $p \in S$ but $p + q \notin S$, so the second cannot be $q - 1$ (and the same holds if we exchange p and q), so there are only 2 choices for such digraphs: that in which all of the values are 1, which is $K_p \square K_q$ (where \square represents the cartesian product), and its complement, in which all of the values are $p - 1$ or $q - 1$. Summing up, we see that $|\text{SDW}(pq)| = 2 \cdot 4^{p-1} + 2 \cdot 4^{q-1} - 2 \cdot 2^{p-1} - 2 \cdot 2^{q-1} - 2$. The result follows.

(2): This follows from (1) by letting q tend to infinity.

(3): Substituting $q = p + c$ into (1) and letting p tend to infinity, we have

$$\lim_{p \rightarrow \infty} \frac{|\text{GW}(pq)|}{|\text{SDW}(pq)|} = \lim_{p \rightarrow \infty} \frac{2^{c-1} - 2^{1-2p}}{2^{-1} + 2^{2c-1} - 2^{-p} - 2^{c-p} - 2^{1-2p}}.$$

Deleting the terms that tend to zero, we are left with

$$\lim_{p \rightarrow \infty} \frac{2^{c-1}}{2^{-1} + 2^{2c-1}} = \frac{2^c}{1 + 2^{2c}},$$

as claimed.

(4): By Theorem 2.5, the automorphism group of a non-normal circulant must either fall into category (1) or category (2). If it falls into category (1) then since $n = p^2$ and the n_i are coprime

there can only be a single factor in the direct product, and since the circulant is non-normal, the factor must be S_{p^2} , so the graph is K_{p^2} or its complement, which are generalized wreath circulants. If it falls into category (2) then by Corollary 2.11, it is a generalized wreath circulant. \square

Notice that if we choose a constant $c \geq 2$ and define $S_c = \{pq : q = p + c\}$ where p and q are prime, then as a consequence of Theorem 4.1(3), since $0 < 2^c/(1 + 2^{2^c}) < \infty$, neither generalized wreath circulant digraphs nor strictly deleted circulant digraphs dominates in S_c . Unfortunately, it is not known whether any set S_c is infinite. Essentially, we have shown that if $n = pq$ is a product of two primes, then generalized wreath products dominate amongst circulant digraphs of order n if $p = q$ (in fact there are no others); neither family dominates if p and q are “close” to each other, and strictly deleted wreath products dominate if one prime is much larger than the other.

We now give two infinite sets S_1 and S_2 of integers, each integer in both sets being divisible by three distinct primes. In S_1 , almost all non-normal circulant digraphs are of strictly deleted wreath type (and S_1 includes all of the square-free integers that are not divisible by 2 or 3). Meanwhile in S_2 , almost all non-normal circulant digraphs are generalized wreath circulant digraphs.

Theorem 4.2 *Let $S_1 = \{n \in \mathbb{N} \mid n \text{ is the product of at least three primes and } q^2 \nmid n \text{ where } q \geq 5 \text{ is the smallest prime divisor of } n\}$. Then,*

$$\lim_{n \in S_1, n \rightarrow \infty} \frac{|\text{SDW}(n)|}{|\text{NonNor}(n)|} = 1$$

PROOF. The first sentence of the proof of Corollary 2.17 notes that for a proper divisor m of n (note since $q \geq 5$ we also have $m \geq 5$), the number of digraphs Γ with $H \times S_m \leq \text{Aut}(\Gamma)$ for some 2-closed group $H \leq S_{n/m}$ is precisely $2 \cdot 4^{n/m-1}$. The maximum number of times that a specific circulant digraph Γ can be counted in $\sum_{m|n} 2 \cdot 4^{n/m-1}$, is $d(n) \leq n$, the number of divisors of n . Thus

$$|\text{DW}(n)| \geq \sum_{m|n} 2 \cdot 4^{n/m-1}/n, \text{ and so by Lemma 2.16, } |\text{NonNor}(n)| \geq \sum_{m|n} 2 \cdot 4^{n/m-1}/n. \text{ By Corollary}$$

2.13, we have that $|\text{GW}(n)| \leq (\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q . Then

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{|\text{GW}(n)|}{|\text{NonNor}(n)|} &\leq \lim_{n \rightarrow \infty} \frac{(\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}}{\sum_{m|n} 2 \cdot 4^{n/m-1}/n} \\ &< \lim_{n \rightarrow \infty} \frac{(\log_2^2 n) 2^{n/(q+2)+n/q}}{4 \cdot 4^{n/q-1}/n} \\ &= \lim_{n \rightarrow \infty} \frac{n(\log_2^2 n) 2^{n/(q+2)}}{2^{n/q}} \\ &= \lim_{n \rightarrow \infty} \frac{n \log_2^2 n}{2^{2n/(q(q+2))}}. \end{aligned}$$

Since $q(q+2) < n^{2/3}$ as q is the smallest prime factor of n , $q^2 \nmid n$, and n has at least 3 prime factors, we have $n/(q(q+2)) > n^{1/3}$, so $\lim_{n \rightarrow \infty} \frac{|\text{GW}(n)|}{|\text{NonNor}(n)|} = 0$. As every non-normal circulant digraph of order n is either a generalized wreath or strictly deleted wreath circulant, the result follows. \square

Theorem 4.3 *For any natural number n , let p_n be the smallest prime divisor of n , and q_n the smallest prime divisor of n such that $q_n \neq p_n$ and $q_n^2 \nmid n$. Let $S_2 = \{n \in \mathbb{N} : p_n \geq 5, p_n^2 \mid n, n \text{ has at least 3 distinct prime divisors, and } q_n > 2p_n\}$. Then*

$$\lim_{n \in S_2, n \rightarrow \infty} \frac{|\text{GW}(n)|}{|\text{NonNor}(n)|} = 1.$$

PROOF. Let $p = p_n$. First notice that there are $2^{p-1+n/p-1}$ circulant digraphs that are wreath products $\Gamma_1 \wr \Gamma_2$ where Γ_1 has order n/p and Γ_2 has order p : 2^{p-1} choices for $S \cap \langle n/p \rangle$ and $2^{n/p-1}$ choices for which cosets of $\langle n/p \rangle$ are in S . All of these digraphs are distinct, so since by Lemma 3.3 these are all non-normal, we have $|\text{NonNor}(n)| \geq 2^{p+n/p-2}$.

By Corollary 2.17, for a proper divisor $m \geq 4$ of n , the number of digraphs of deleted wreath type is at most $4^{n/m}$. Thus $|\text{DW}(n)| \leq \sum_{m \mid n, \gcd(m, n/m)=1} 4^{n/m}$. Let $\prod_{i=1}^t p_i^{a_i}$ be the prime decomposition of n , and let $p_k^{a_k} = \min_{1 \leq i \leq t} \{p_i^{a_i}\}$. Clearly $4^{n/(p_k^{a_k})}$ is the largest term in this sum, and there are at most $d(n)$ (the number of divisors of n) terms in this sum. Thus $|\text{DW}(n)| \leq d(n) \cdot 4^{n/(p_k^{a_k})}$.

Observe that if $a_k \geq 2$, then $p_k^{a_k} \geq 5p > 2p$ since $p \geq 5$ is the smallest divisor of n . Also, if $a_k = 1$, then by hypothesis $p_k \geq q_n > 2p$. Hence $p_k^{a_k} - 2p \geq 1$ since both are integers. Now,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{|\text{DW}(n)|}{|\text{NonNor}(n)|} &\leq \lim_{n \rightarrow \infty} \frac{d(n) \cdot 4^{n/(p_k^{a_k})}}{2^{p+n/p-2}} \\ &= \lim_{n \rightarrow \infty} \frac{4d(n)}{2^{p+n/p-2n/(p_k^{a_k})}} \\ &< \lim_{n \rightarrow \infty} \frac{4n}{2^{p+n \cdot (p_k^{a_k}-2p)/(pp_k^{a_k})}} \\ &\leq \lim_{n \rightarrow \infty} \frac{4n}{2^{p+n/(pp_k^{a_k})}}. \end{aligned}$$

Since n has at least 3 distinct prime divisors, there is some j such that $p_j \neq p, p_k$. Now $p_j^{a_j} > p_k^{a_k}$ by our choice of k , and $p_j^{a_j} \geq p_j > p$, so since $n/(pp_k^{a_k}) \geq p_j^{a_j}$, we have $(n/(pp_k^{a_k}))^2 \geq pp_k^{a_k}$. Hence $pp_k^{a_k} \leq n^{2/3}$, so $n/(pp_k^{a_k}) \geq n^{1/3}$. So the above limit is at most

$$\lim_{n \rightarrow \infty} \frac{4n}{2^{p+n^{1/3}}} = 0.$$

\square

References

- [1] Brian Alspach, *Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree*, J. Combinatorial Theory Ser. B **15** (1973), 12–17. MR MR0332553 (48 #10880)
- [2] László Babai and Chris D. Godsil, *On the automorphism groups of almost all Cayley graphs*, European J. Combin. **3** (1982), no. 1, 9–15. MR MR656006 (84d:05092)
- [3] Peter J. Cameron, Michael Giudici, Gareth A. Jones, William M. Kantor, Mikhail H. Klin, Dragan Marušič, and Lewis A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. (2) **66** (2002), no. 2, 325–333. MR MR1920405 (2003f:20001)
- [4] Edward Dobson, *Asymptotic automorphism groups of Cayley digraphs and graphs of abelian groups of prime-power order*, Ars Math. Contemp. **3** (2010), no. 2, 200–213. MR 2739429
- [5] Edward Dobson and Joy Morris, *On automorphism groups of circulant digraphs of square-free order*, Discrete Math. **299** (2005), no. 1-3, 79–98. MR MR2168697 (2006m:20004)
- [6] S. A. Evdokimov and I. N. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra i Analiz **14** (2002), no. 2, 11–55. MR MR1925880 (2003h:20005)
- [7] Ka Hin Leung and Shing Hing Man, *On Schur rings over cyclic groups. II*, J. Algebra **183** (1996), no. 2, 273–285. MR MR1399027 (98h:20009)
- [8] ———, *On Schur rings over cyclic groups*, Israel J. Math. **106** (1998), 251–267. MR MR1656873 (99i:20009)
- [9] Cai Heng Li, *Permutation groups with a cyclic regular subgroup and arc transitive circulants*, J. Algebraic Combin. **21** (2005), no. 2, 131–136. MR MR2142403 (2006b:20002)
- [10] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, lectures given at The Ohio State University, Columbus, Ohio, 1969.
- [11] Helmut Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964. MR MR0183775 (32 #1252)
- [12] ———, *Mathematische Werke/Mathematical works. Vol. 1*, Walter de Gruyter & Co., Berlin, 1994, Group theory, With essays on some of Wielandt’s works by G. Betsch, B. Hartley, I. M. Isaacs, O. H. Kegel and P. M. Neumann, Edited and with a preface by Bertram Huppert and Hans Schneider. MR MR1272467 (95b:01025)

- [13] Ming-Yao Xu, *Automorphism groups and isomorphisms of Cayley digraphs*, Discrete Math. **182** (1998), no. 1-3, 309–319, Graph theory (Lake Bled, 1995). MR MR1603719 (98i:05096)